手 続 補 正 書
（法第１１条の規定による補正）

特 許 庁 長 官　殿

１．国際出願の表示　ＰＣＴ／ＪＰ２００４／００３５２０

２．出願人
名　　称　セイコーエプソン　株式会社
SEIKO EPSON CORPORATION
あ て 名　〒163-0811 日本国東京都新宿区西新宿二丁目４番１号
4-1, Nishishinjuku 2-chome, Shinjuku-ku
Tokyo 1630811 Japan
国　　籍　日本国　Japan
住　　所　日本国　Japan

３．代理人
名　　称　特許業務法人湘洋内外特許事務所
The Patent Corporate Body ShowYou International
あ て 名　〒220-0004 日本国神奈川県横浜市西区北幸２丁目９－１０
横浜ＨＳビル　７階
7F, Yokohama HS-Bldg., 9-10, Kitasaiwai 2-chome,
Nishi-ku, Yokohama-shi, Kanagawa 220-0004, Japan
代 表 者　三 品 岩 男　MISHINA Iwao

４．補正の対象　請求の範囲

５．補正の内容
（１）　出願時の請求の範囲第１項第３行目から第６行目「ネットワークを介してアクセス可能なおとりを、ウィルスの進入を監視するコンピュータ上に設けて、ネットワークを介して前記おとりに対するアクセスを受け付けて、通信情報を取得すると共に、ウィルスの侵入を検出し、そのおとりにウィルスが侵入した時、対応して、」を、「ウィルスが侵入したとき通信情報を取得し、」と補正する。
（２）　出願時の請求の範囲第１項第９行目「ウィルス攻撃処理を行なうこと、」を、「ウィルス攻撃処理を行うことを予告するメッセージを送信し、当該ウィ

ルスの送信元となっているコンピュータに対して、ウィルス攻撃処理を行うこと」と補正する。

（３）　出願時の請求の範囲第２項第１行目と第２行目との間に、「ネットワークを介してアクセス可能なおとりを、ウィルスの侵入を監視するコンピュータ上に設けて、ネットワークを介して前記おとりに対するアクセスを受け付けて、通信情報を取得すると共に、ウィルスの侵入を検出し、」を挿入する。

（４）　出願時の請求の範囲第６項第３行目から第４行目「ネットワークを介してアクセスが可能なおとり手段と、前記おとり手段へのウィルスの侵入を検出し、」を、「ウィルスの侵入を検出し、」と補正する。

（５）　出願時の請求の範囲第６項第８行目から第９行目「コンピュータ攻撃手段と、」を、「コンピュータ攻撃手段と、感染したコンピュータに対して、攻撃開始を予告するためのメッセージを送信する手段と、」と補正する。

（６）　出願時の請求の範囲第７項第２行目から第４行目「前記おとり手段は、おとりフォルダを記憶装置に記憶させたもの、おとりアプリケーションを記憶装置に記憶させたもの、および、記憶装置に擬似的に形成したサーバ、のうち１以上である」を、「ネットワークを介してアクセスが可能なおとり手段をさらに備え、前記通信情報解析手段は、前記おとり手段へのウィルスの侵入を検出し、かつ、ウィルスの侵入を検出した時、ウィルスの侵入時に取得した通信情報から当該ウィルスの送信元となっているコンピュータを検出するものである」と補正する。

（７）　出願時の請求の範囲第９項第第４行目「方法」を、「システム」と補正する。

（８）　出願時の請求の範囲第１１項第１行目「請求項８、」を、「請求項６，７，８、」と補正する。

（９）　出願時の請求の範囲第１４項を削除する。

（１０）出願時の請求の範囲第１５項第１行目「請求項８、」を、「請求項６，７，８、」と補正する。

（１１）出願時の請求の範囲第１６項第１行目「請求項８、」を、「請求項６，７，８、」と補正する。

（１２）出願時の請求の範囲第１８項第１行目「ネットワークでのウィルスの感染を検出して、ウィルスの感染の阻止をコンピュータに実行させるプログラムであって、予め設けられたネットワークを介してアクセスが可能なおとり手段へのウィルスの侵入を検出し、」を、「ウィルスの侵入を検出し、」と補正する。

（１３）出願時の請求の範囲第１８項第８行目から第９行目「コンピュータ攻撃手段とをコンピュータに構築させる、」を、「コンピュータ攻撃手段と、感染したコンピュータに対して、攻撃開始を予告するためのメッセージを送信する手

段と、をコンピュータに構築させる、」と補正する。

（１４） 出願時の請求の範囲第１９項を削除する。

（１５） 請求の範囲第２０項「ネットワークでのウィルスの感染を検出して、ウィルスの感染を阻止するシステムであって、ウィルスの侵入を検出し、かつ、ウィルスの侵入を検出した時、ウィルスの侵入時に取得した通信情報から当該ウィルスの送信元となっているコンピュータを検出する通信情報解析手段と、ウィルスの送信元となっているコンピュータに対して、ネットワークを介してウィルスの活動を抑制するウィルス攻撃処理を行うコンピュータ攻撃手段と、攻撃開始時もしくは攻撃開始以後、攻撃元の端末装置で警報音を発生する手段と、備えることを特徴とするウィルスの感染を阻止するシステム。」を追加する。

（１６） 請求の範囲第２１項「ネットワークでのウィルスの感染を検出して、ウィルスの感染を阻止するシステムであって、ウィルスの侵入を検出し、かつ、ウィルスの侵入を検出した時、ウィルスの侵入時に取得した通信情報から当該ウィルスの送信元となっているコンピュータを検出する通信情報解析手段と、ウィルスの送信元となっているコンピュータの管理者宛の検出報告を発する手段と、を備えることを特徴とするウィルスの感染を阻止するシステム。」を追加する。

６．添付書類の目録

（１）請求の範囲第１８頁から２２頁及び２２／１頁

請求の範囲

１．（補正後）　ネットワークでのウィルスの感染を検出して、ウィルスの感染を阻止する方法であって、

ウィルスが侵入したとき通信情報を取得し、取得した通信情報に基づいて、ウィルスの送信元となっているコンピュータを検出し、ウィルスの送信元となっているコンピュータに対して、ネットワークを介してウィルスの活動を抑制するウィルス攻撃処理を行うことを予告するメッセージを送信し、当該ウィルスの送信元となっているコンピュータに対して、ウィルス攻撃処理を行うことを特徴とするウィルスの感染を阻止する方法。

２．（補正後）　請求項１に記載のウィルスの感染を阻止する方法において、

ネットワークを介してアクセス可能なおとりを、ウィルスの侵入を監視するコンピュータ上に設けて、ネットワークを介して前記おとりに対するアクセスを受け付けて、通信情報を取得すると共に、ウィルスの侵入を検出し、

前記おとりは、おとりフォルダを記憶装置に記憶させたもの、おとりアプリケーションを記憶装置に記憶させたもの、および、記憶装置に擬似的に形成したサーバ、のうち１以上であるウィルスの感染を阻止する方法。

３．　請求項１に記載のウィルスの感染を阻止する方法において、

前記ウィルス攻撃は、前記ウィルスの送信元となっているコンピュータに高負荷を与えるものであるウィルスの感染を阻止する方法。

４．　請求項３に記載のウィルスの感染を阻止する方法において、

前記ウィルスの送信元となっているコンピュータに与える高負荷は、

当該コンピュータのトラフィックを増大させることであるウィルスの感染を阻止する方法。

5．　請求項3に記載のウィルスの感染を阻止する方法において、

前記ウィルスの送信元となっているコンピュータに与える高負荷は、当該コンピュータのＣＰＵが応答動作をすべき処理を大量に要求することであるウィルスの感染を阻止する方法。

6．（補正後）　ネットワークでのウィルスの感染を検出して、ウィルスの感染を阻止するシステムであって、

ウィルスの侵入を検出し、かつ、ウィルスの侵入を検出した時、ウィルスの侵入時に取得した通信情報から当該ウィルスの送信元となっているコンピュータを検出する通信情報解析手段と、

ウィルスの送信元となっているコンピュータに対して、ネットワークを介してウィルスの活動を抑制するウィルス攻撃処理を行うコンピュータ攻撃手段と、

感染したコンピュータに対して、攻撃開始を予告するためのメッセージを送信する手段と、

を備えることを特徴とするウィルスの感染を阻止するシステム。

7．（補正後）　請求項6に記載のウィルスの感染を阻止するシステムにおいて、

ネットワークを介してアクセスが可能なおとり手段をさらに備え、

前記通信情報解析手段は、前記おとり手段へのウィルスの侵入を検出し、かつ、ウィルスの侵入を検出した時、ウィルスの侵入時に取得した通信情報から当該ウィルスの送信元となっているコンピュータを検出するものであるウィルスの感染を阻止するシステム。

8．　請求項6に記載のウィルスの感染を阻止するシステムにおいて、

前記コンピュータ攻撃手段は、前記ウィルスの送信元となっているコンピュータに高負荷を与えるものであるウィルスの感染を阻止するシステム。

９．（補正後）　請求項８に記載のウィルスの感染を阻止するシステムにおいて、

前記コンピュータ攻撃手段は、前記ウィルスの送信元となっているコンピュータのトラフィックを増大させて、当該コンピュータ高負荷を与えることであるウィルスの感染を阻止するシステム。

１０．　請求項８に記載のウィルスの感染を阻止するシステムにおいて、

前記コンピュータ攻撃手段は、前記ウィルスの送信元となっているコンピュータのＣＰＵが応答動作をすべき処理を大量に要求して、当該コンピュータに高負荷を与えることであるウィルスの感染を阻止するシステム。

１１．（補正後）　請求項６、７、８、９および１０のいずれか一項に記載のウィルスの感染を阻止するシステムにおいて、

ウィルスの送信元となっているコンピュータの管理者宛の検出報告を発する手段をさらに備え、

前記コンピュータ攻撃手段は、当該ウィルスへの対策が完了するまで、当該コンピュータへの攻撃を継続するウィルスの感染を阻止するシステム。

１２．　請求項６に記載のウィルスの感染を阻止するシステムにおいて、

前記おとり手段は、ネットワークに接続されたコンピュータの記憶装置上に擬似的に形成した、おとりサーバ中に設けられたアプリケーショ

ンにより構成されるおとりフォルダであるウィルスの感染を阻止するシステム。

１３．　請求項６に記載のウィルスの感染を阻止するシステムにおいて、

前記おとり手段は、ネットワークに接続されたコンピュータの記憶装置上に擬似的に形成した、おとりサーバ中に設けられたアプリケーションにより構成されるおとりアプリケーションであるウィルスの感染を阻止するシステム。

１４．（削除）

１５．（補正後）　請求項６、７、８、９および１０のいずれか一項に記載のウィルスの感染を阻止するシステムにおいて、

攻撃開始時もしくは攻撃開始以後、攻撃元の端末装置で警報音を発生する手段をさらに備えるウィルスの感染を阻止するシステム。

１６．（補正後）　請求項６、７、８、９および１０のいずれか一項に記載のウィルスの感染を阻止するシステムにおいて、

ネットワークに接続された別のコンピュータに対して、ウィルス送信元となっているコンピュータのネットワークアドレスを通知するとともに、ウィルスの送信元となっているコンピュータに対してウィルス攻撃処理を行うことを依頼する手段をさらに備えるウィルスの感染を阻止するシステム。

１７．　ネットワークでのウィルスの感染を検出して、ウィルスの感染を阻止するシステムであって、

ウィルスの送信元となっているコンピュータに対してウィルス攻撃処理を行うことについての依頼を受ける手段と、

前記受けた依頼に基づいて、前記ウィルスの送信元となっているコンピュータに対して、ネットワークを介してウィルスの活動を抑制するウィルス攻撃処理を行うコンピュータ攻撃手段と、を備えることを特徴とするウィルスの感染を阻止するシステム。

１８．（補正後）　ウィルスの侵入を検出し、かつ、ウィルスの侵入を検出した時、ウィルスの侵入時に取得した通信情報から当該ウィルスの送信元となっているコンピュータを検出する通信情報解析手段と、

ウィルスの送信元コンピュータに対して、ネットワークを介してウィルスの活動を抑制するウィルス攻撃処理を行うコンピュータ攻撃手段と、

感染したコンピュータに対して、攻撃開始を予告するためのメッセージを送信する手段と、をコンピュータに構築させる、ウィルスの感染を阻止するプログラム。

１９．（削除）

２０．（追加）　ネットワークでのウィルスの感染を検出して、ウィルスの感染を阻止するシステムであって、

ウィルスの侵入を検出し、かつ、ウィルスの侵入を検出した時、ウィルスの侵入時に取得した通信情報から当該ウィルスの送信元となっているコンピュータを検出する通信情報解析手段と、

ウィルスの送信元となっているコンピュータに対して、ネットワークを介してウィルスの活動を抑制するウィルス攻撃処理を行うコンピュータ攻撃手段と、

攻撃開始時もしくは攻撃開始以後、攻撃元の端末装置で警報音を発生する手段と、

を備えることを特徴とするウィルスの感染を阻止するシステム。

２１．（追加）　ネットワークでのウィルスの感染を検出して、ウィルスの感染を阻止するシステムであって、

ウィルスの侵入を検出し、かつ、ウィルスの侵入を検出した時、ウィルスの侵入時に取得した通信情報から当該ウィルスの送信元となっているコンピュータを検出する通信情報解析手段と、

ウィルスの送信元となっているコンピュータの管理者宛の検出報告を発する手段と、を備えることを特徴とするウィルスの感染を阻止するシステム。

答　　弁　　書

特　許　庁　長　官　　殿

1．国際出願の表示　　ＰＣＴ／ＪＰ２００４／００３５２０

2．出願人

名　　称　　セイコーエプソン　株式会社
SEIKO EPSON CORPORATION

あ　て　名　　〒163-0811 日本国東京都新宿区西新宿二丁目４番１号
4-1, Nishishinjuku 2-chome, Shinjuku-ku
Tokyo 1630811 Japan

国　　籍　　日本国　　Japan

住　　所　　日本国　　Japan

3．代理人

名　　称　　特許業務法人湘洋内外特許事務所
The Patent Corporate Body ShowYou International

あ　て　名　　〒220-0004 日本国神奈川県横浜市西区北幸２丁目９－１０
横浜ＨＳビル　７階
7F, Yokohama HS-Bldg., 9-10, Kitasaiwai 2-chome,
Nishi-ku, Yokohama-shi, Kanagawa 220-0004, Japan

代　表　者　　三　品　岩　男　　MISHINA Iwao

4．通知の日付　　１１．５．２００４

５．答弁の内容

本願に対し国際調査機関の見解書が出されました。それによりますと、本願の請求の範囲１－１０、１２、１３、１６－１９について進歩性なしとの見解が示されています。同日に提出した手続補正書により、請求の範囲について補正を行いました。これにより、補正後の請求の範囲は、すべて進歩性を有するものになったと考えます。

１．請求の範囲１、２、６、７および１８について

補正前の請求の範囲１に、“ウィルスの送信元となっているコンピュータに対して、ネットワークを介してウィルスの活動を抑制するウィルス攻撃処理を行うことを予告するメッセージを送信”することを加える補正を行いました。加えた事項は、補正前の請求項１４に記載されていた事項であって、見解書において進歩性ありとの見解が示されている事項です。同様の補正を請求の範囲６および１８についても行っています。従って、請求の範囲１および１８は、進歩性があるものと考えます。

なお、請求の範囲１において記載されていた“ネットワークを介してアクセス可能なおとりを、ウィルスの侵入を監視するコンピュータ上に設けて、ネットワークを介して前記おとりに対するアクセスを受け付けて、通信情報を取得すると共に、ウィルスの侵入を検出し、”を請求の範囲２に移す補正を行いました。また、補正前の請求の範囲６に記載されていた同様の事項ついて請求の範囲７に移す補正を行いました。

２．請求の範囲２０について

請求の範囲２０を追加しました。請求の範囲２０は、補正前の請求の範囲１５に記載される事項に、補正前の請求の範囲６に記載される事項の一分を加えて独立項としたものです。補正前の請求の範囲１５に記載される警報については、進歩性が肯定されています。

３．請求の範囲２１について

請求の範囲２１を追加しました。請求の範囲２１は、補正前の請求の範囲１１に記載される事項の一部に、補正前の請求の範囲６に記載される事項の一部を加えて独立項としたものです。補正前の請求の範囲１１

に記載される検出方向を発する手段については、進歩性が肯定されていると考えます。

４．むすび

以上に述べましたように、補正後の請求の範囲は、そのすべてにおいて、見解書において進歩性が肯定されている事項を含むこととなりました。従って、補正後の請求の範囲については、進歩性があると考えます。